Electronic Frontiers
AUSTRALIA

Submission to the Senate Standing Committee on Environment, Communications and the Arts inquiry into the adequacy of protections for the privacy of Australians

Introduction

Electronic Frontiers Australia Inc. (EFA) is a non-profit national organisation representing Internet users concerned with on-line rights and freedoms. EFA was established in 1994, is independent of government and commerce, and is funded by membership subscriptions and donations from individuals and organisations with an altruistic interest in promoting online civil liberties.

In this submission we wish to concern ourselves with the privacy impacts of potential data retention laws on Australians.

In recent months, it has come to the public's attention that the Attorney General's Department has consulted with industry on the possible outlines of a mandatory data retention regime. That is, through legislation or regulation, requiring telecommunications companies to maintain a database of information about the communications of their customers for the benefit of law enforcement agencies who may requisition it when investigating criminal activity. It is understood that this work is being taken in preparation to the possible accession of Australia to the European Convention on Cybercrime treaty.

Any possible scheme involving the private communications of Australian citizens has enormous privacy implications. EFA feels it is necessary that privacy considerations be given sufficient consideration next to the requirements, or supposed requirements, of police.

In this submission, we outline some of the considerations surrounding this aspect of data collection activities of government agencies.

1. Information on proposed regulation

On June 16th, 2010, ZDNet reported that the Attorney-General's Department had been involved in consultations with industry on the subject of implementing a data retention regime.[1] According to the same article, an industry source expressed alarm at both the scope of the proposed scheme and the amount of time data would be kept. "We're talking browsing history and emails, way beyond what I would consider to be normal SMS, retaining full browsing history and everything," said the source.

---

[1] http://www.zdnet.com.au/govt-wants-isps-to-record-browsing-history-339303785.htm

The AG's Department has refused to release any substantive information on their plans. Documents requested under Freedom of Information laws were very heavily censored and shed no light on the process.[2] Reports indicate that the terrorists and pedophilia were mentioned, with no details discussed on how data retention might aid in the prevention of such crimes.

Information available at the present time suggests that a data retention scheme remains on the Government's agenda and if pursued will be done so aggressively. We therefore think it crucial that a full and frank public debate and consultation be conducted, so that the many real and serious issues surrounding such a scheme are given due consideration.

2. Overseas situation

Several jurisdictions around the world have data retention laws requiring telecommunications providers to record data about their customers communications. This sets a precedent that Australia appears set to follow, but can also be instructive where it has generated significant controversy.

The European Union's data retention regime was set in place with the adoption of Directive 2006/24/EC, on "the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC".[3] The Directive covers fixed, mobile and internet telephony and Internet access and email communications. Member states are required to craft legislation that mandates the retention for between 6 months and 2 years of enough information to determine the type, location, time, duration and destination of a communication. This amounts to enormous amounts of information.

The scheme has attracted significant controversy. As of the beginning of 2010, only 17 of the 31 countries had fully implemented the Directive. In March this year, Germany's Federal Constitution Court suspended the German law implementing the Directive, ruling it was unconstitutional.[4] Among other reasons, they cited a lack of transparency in the potential uses of the data.[5] Meanwhile, Sweden has faced sanctions for failing to comply.[6]

In contrast, countries such as Italy and Ireland have implemented even more stringent laws.[7]

---

[2]http://www.smh.com.au/technology/technology-news/no-minister-90-of-web-snoop-document-censored-to-stop--premature-unnecessary-debate-20100722-10mxo.html

[3]http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:EN:PDF

[4]http://www.readwriteweb.com/archives/germanys_supreme_court_suspends_data_retention_law.php

[5]http://www.bverfg.de/pressemitteilungen/bvg10-011en.html

[6]http://www.crn.com.au/News/215135,lessons-learned-from-europes-data-retention-laws.aspx

[7]http://en.wikipedia.org/wiki/Telecommunications_data_retention#Italy

In the USA, no similar scheme exists. One bill, the Internet Stopping Adults Facilitating the Exploitation of Today's Youth (SAFETY) Act of 2009, currently making its way through Congress, mandates that Internet service providers maintain records of the identity of users associated with IP addresses for two years.[8]

3. Benefits to law enforcement

The ostensible justification for a mandatory data retention scheme is to benefit police investigating criminal activity both online and offline. EFA feels that far from being obvious, the benefits for crime fighting are highly questionable. To justify the advent of what amounts to widespread surveillance of the Australian public, a detailed case must be made that current sources of information are inadequate for the prosecution of certain crimes. EFA does not believe that crime "prevention" can be used to justify a system that would collect data on the entire population, regardless of whether they are suspected of a crime or not.

According to media reports, even the Australian Federal Police have called into question the effectiveness of a data retention scheme as proposed by the Attorney General. According to ComputerWorld, Neil Gaughan, the National manager of the AFP High Tech Crime Operations and Assistant Commissioner, said "the regime revealed earlier this year would have little effect on how the AFP curbed crime."[9]

It is worth noting that determined criminals will have little difficulty disguising or anonymising their communications. It is therefore highly questionable whether a new and broad data retention scheme would aid in the investigation of terrorism, organised crime, and so on.

EFA feel that any move to introduce data retention laws that could negatively impact the privacy of Australian citizens should begin with a detailed accounting of how this scheme will bring tangible benefits to the community through a reduction in crime. Clearly, a law of diminishing returns applies as the volume of data recorded about the public's communications increases.

4. Transparency

EFA feels very strongly that any proposal for a data retention scheme must be dealt with as transparently as possible. Firstly, with regards to the implementation of the scheme, EFA feel that the Australian public should be consulted from the beginning. The idea that discussion "may lead to premature unnecessary debate and could potentially prejudice and impede government decision making", cited as one reason for refusing to release information under Freedom of Information, is not compatible with an open democracy.[10]

---

[8]http://www.govtrack.us/congress/bill.xpd?bill=h111-1076

[9]http://www.computerworld.com.au/article/359713/data_retention_fine_it_afp/

[10]http://www.smh.com.au/technology/technology-news/no-minister-90-of-web-snoop-document-censored-to-stop--premature-unnecessary-debate-20100722-10mxo.html

Secondly, in operation the scheme must be as transparent as possible as well, so that members of the public are able to be fully aware of which aspects of their communications may be recorded. EFA does not accept that such transparency would somehow aid criminals or put Australians at risk.

5. Privacy issues

The biggest concern with a mandatory data retention regime is the threat to Australians' right to privacy. Our communications with business, colleagues, friends and loved ones are among the most sensitive information any of us will generate in our daily lives. A data retention scheme would threaten this privacy in a number of ways.

Firstly, the widespread existence of large databases of customer communications almost guarantees that a leak will occur at some point in the future. Given all ISPs, from the largest and most sophisticated to the smallest single-person operations would come under the jurisdiction of the law, security measures will differ in quality, and even the most well-resourced companies can have data breaches. Although the contents of the communications would not be recorded, the consequences of such a breach could be catastrophic for individuals whose data is exposed. Already, we appreciate how a leak of mobile phone billing records could expose sensitive relationships. This risk will be compounded when the number of companies required to collect information is increased, along with the types of communications and volumes of data.

Regardless of legal protections surrounding access to the data, the existence of the information would also potentially be subject to access by persons inside the companies where the data is collected. This could occur for personal reasons, or, for instance, as part of a company policy to analyse the data for marketing or other purposes.

In its decision striking down the German law, Germany's Federal Constitutional Court noted:

> "Even though the storage does not extend to the contents of the communications, these data may be used to draw content-related conclusions that extend into the users' private sphere... The observation over time of recipient data, dates, times and the place of phone conversations, it continued, "permit detailed information to be obtained on social or political affiliations and on personal preferences, inclinations and weaknesses." [11]

While Australians enjoy no explicit legal or constitutional right to privacy, the reasonable expectation by Australians is that their daily lives, of which electronic communications form an increasing part, should be free from arbitrary interference or monitoring by government. EFA believes that most Australians would greet the proposed system with suspicion and alarm at the threat it poses to their privacy. This should also be a factor in any decision to legislate in this area.

---

[11] http://www.bverfg.de/pressemitteilungen/bvg10-011en.html

6. Potential for abuses

The existence of a database of communication activity raises the potential for abuse by governments and police. While we can earnestly hope that sufficient checks and balances would exist to prevent authorities abusing such databases to gather information on protesters (for instance), the only way to ensure that this never happens is to prevent the data being collected in the first place.

Germany's Federal Constitutional Court wrote:

> "Depending on the use of the telecommunication, such storage can make it possible to create meaningful personality profiles of virtually all citizens and track their movements. It also increases the risk of citizens to be exposed to further investigations without themselves having given occasion for this. In addition, the possibilities of abuse that are associated with such a collection of data aggravate its burdensome effect. In particular since the storage and use of data are not noticed, the storage of telecommunications traffic data without occasion is capable of creating a diffusely threatening feeling of being watched which can impair a free exercise of fundamental rights in many areas."[12]

EFA is also concerned that should such a system be put in place, the scope of acceptable uses would be too broad or would be broadened in response to political pressure. For instance, that collected data would be made available for use in civil proceedings relating to alleged copyright infringement.

EFA feels that any proposal for the introduction of a mandatory data retention scheme should weigh the potential for abuse against any supposed benefits the scheme will bring to the public.

7. Costs to service providers

An aggressive data retention regime would place a significant burden on communications companies including retail internet service providers. ISPs log certain types of data as part of their normal operations and for the purposes of billing or providing other services. However, maintaining records of all accessible data for long periods of time, as well as servicing law enforcement requests to access the data, would impose costs far and above those of normal operations.

According to the UK Internet Service Providers' Association one large UK-based ISP estimates that it would cost £26m a year to set up a data retention system along with 9m a year in running costs.[13]

---

[12] http://www.bverfg.de/pressemitteilungen/bvg10-011en.html

[13] http://www.theregister.co.uk/2005/12/14/eu_data_retention_vote/

Summary

The mandatory data retention scheme which is apparently being sought by the Attorney General presents a clear threat to Australians' privacy. An enormous corpus of extremely sensitive data would be collected on every inhabitant of the country. This data could be exposed accidentally or maliciously and would be open to abuse by private individuals, law enforcement and governments. The existence of such a scheme, we believe, would also have a corrosive effect on Australians' faith and trust in government.

In order to safeguard the privacy of Australians' communications, any scheme under consideration should be tightly constrained:

- Short horizons for expiry of data, such as 90-180 days
- Strict restrictions on access, and access only under judicial order
- Data that is part of the contents of communications (such as an email subject line) must be excluded
- Protocols and data covered by the scheme should be strictly limited to that with a demonstrated use in prosecution of serious crimes, not a blanket order to ISPs to save "all logged data".
- Email communications should be excluded, at the very least unless the service provider is the primary host of the email accounts in question
- Web browsing history should not be included
- Data may not be used for civil purposes, such as copyright enforcement
- Secure destruction of data should be mandated after the expiry of retention timelines.

Finally, we reiterate the need for a transparent and consultative process in deliberating on any such scheme.

For further information please contact us.

Colin Jacobs
Chair

Appendix: About EFA

Electronic Frontiers Australia Inc. (EFA) is a non-profit national organisation representing Internet users concerned with on-line freedoms and rights. EFA was established in January 1994 and incorporated under the Associations Incorporation Act (S.A.) in May 1994.

EFA is independent of government and commerce and is funded by membership subscriptions and donations from individuals and organisations with an altruistic interest in promoting online civil liberties.

Our major objectives are to protect and promote the civil liberties of users and operators of computer based communications systems such as the Internet, to advocate the amendment of

laws and regulations in Australia and elsewhere (both current and proposed) which restrict free speech and to educate the community at large about the social, political, and civil liberties issues involved in the use of computer based communications systems.

EFA members and supporters come from all parts of Australia and from diverse backgrounds. They are people who recognise that preserving freedoms and rights always depends on the willingness of people to defend them and that combatting the threats posed by the anti-civil libertarian forces, the radical right agenda and ill-informed reports in the media requires constant vigilance and support.